AMENDMENTS TO THE CLAIMS

Please amend the claims by replacing the original claims with the following listing of claims.

LISTING OF THE CLAIMS:

1. (Currently Amended) A software virus detection method, comprising:

- interpreting code that is suspected of containing proscribed code with an interpreter;

- evaluatively writing with said interpreter the results of said interpretation;

- scanning the results of said interpretation for the presence of proscribed code and identifying proscribed code in said results, and making said results available to a reporter for reporting or to a processor for further processing of said results with a processing component.

2. (Previously presented) The method of claim 1, wherein scanning the results of said interpretation for the presence of proscribed code further comprises scanning for the presence of code of interest.

3. (Previously presented) The method of claim 2, wherein scanning for the presence of code of interest further comprises scanning for a file open command or a file modify command.

4. (Previously presented) The method of claim 2, wherein scanning the results of said interpretation for the presence of proscribed code further comprises scanning for the presence of proscribed code of interest.

5. (Previously presented) The method of claim 4 wherein scanning for the presence of proscribed code of interest further comprises scanning for viral code or viral patterns.

6. (Original) A software virus detection article of manufacture comprising: a computer readable medium; and, a table of interpreted results, comprising interpreted proscribed code.

7. (Previously presented) A software virus detection apparatus, comprising: an evaluative code interpreter; a pattern analyzer; a results evaluator; a reporter; whereby, after proscribed code is interpreted by said evaluative code interpreter and results generated, those results are reviewed by said pattern analyzer for the presence of proscribed code, and results reported to said results evaluator, and from said results evaluator to a reporter.

8. (Previously presented) The apparatus of claim 7, wherein said evaluative code

interpreter further reviews said code for the presence of code of interest.

9. (Previously presented) The apparatus of claim 8, wherein said evaluative code interpreter further reviews said code for the presence of a file open command or a file modify command.

10. (Previously presented) The apparatus of claim 9,wherein said pattern analyzer further reviews said code for the presence of code of interest.

11. (Previously presented) The apparatus of claim 10, wherein said pattern analyzer further reviews said code for the presence of proscribed code.

12. (Previously presented) The apparatus of claim 11, wherein said pattern analyzer further reviews said code for the presence of viral code or viral patterns.

13. (New) A software virus detection method, comprising:

- interpreting code that is suspected of containing proscribed code with an interpreter, wherein said interpreter includes a plurality of facilities for facilitating the interpretation of a plurality of code formats and languages in source or compiled form;
- evaluatively writing with said interpreter the results of said interpretation, wherein said results of said interpretation consist of a summarily evaluation of said suspect code;

- scanning the results of said interpretation for the presence of proscribed code and identifying proscribed code in said results, and making said results available to a reporter for reporting or to a processor for further processing of said results with a processing component.

14. (New). The method of claim 13, including ascertaining in said suspect code the presence of one or more instructions selected from the group consisting of file open write and file open modify;

setting a pointer in a code sequence containing said one or more instructions;

setting an emergency flag;

sending to a reporter an emergency message; and

communicating an alert from said reporter to a recipient.